

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TAYLOR SMITH,
Plaintiff,
v.
YETI COOLERS, LLC,
Defendant.

Case No. 24-cv-01703-RFL

**ORDER GRANTING MOTION TO
DISMISS WITH LEAVE TO AMEND**

Re: Dkt. No. 23

Plaintiff Taylor Smith alleges that Defendant YETI Coolers, LLC uses a third-party payment processor, Adyen, to process customer purchases on its website, and that Adyen incorporates customers' financial information into its fraud prevention system, which it then markets to merchants without customers' consent. Plaintiff alleges that this constitutes an interception of their sensitive information by Adyen with Defendant's assistance and invades their privacy. Plaintiff now brings this putative class action under the California Invasion of Privacy Act, for violations of California Penal Code §§ 631(a) and 632, and under California's Constitution, for invasion of privacy. Defendant's motion to dismiss is **GRANTED WITH LEAVE TO AMEND**, for the reasons further detailed below. The operative complaint does not sufficiently allege Defendant's knowledge of Adyen's allegedly wrongful conduct or Defendant's intent to assist Adyen in that conduct. Because it is not clear whether Plaintiff could cure this defect through amendment, the dismissal is with leave to amend.

I. ALLEGATIONS OF FIRST AMENDED COMPLAINT

Defendant owns and operates the YETI website, www.yeti.com, which sells YETI-brand products for purchase. To facilitate the payment process, Defendant engaged a third-party company, Adyen. Defendant integrated Adyen's online payment processing platform into its

website “for the purported purpose of processing consumer purchases” and “protect[ing] Defendant from fraudulent transactions.” (Dkt. No. 21 (“First Amended Complaint” or “FAC”) ¶¶ 24, 34.)

But according to Plaintiff, these are not the only services that Adyen provides. Rather, Adyen “intercepts and indefinitely stores consumers’ [personally identifiable information] and financial information into its fraud prevention network,” which Adyen uses to provide additional risk management services to merchants. (*Id.* ¶¶ 25-26.) By accessing Adyen’s network, merchants are able to “gain valuable insights into consumers’ purchasing history by tracking and recording consumers’ purchases across devices and networks.” (*Id.* ¶ 30.) Plaintiff further alleges that nowhere on Defendant’s website is there information to alert consumers that a third party is involved in payment processing and that their sensitive information is being “shared with and indefinitely stored by a third party.” (*Id.* ¶¶ 35-37.) And according to Plaintiff, nor have consumers consented to the disclosure of this information. (*Id.* ¶ 42.)

Plaintiff alleges that this conduct amounts to the illegal recording of confidential communications, in violation of Sections 631(a) and 632 of the California Invasion of Privacy Act, and an illegal invasion of privacy under the California Constitution. And, according to Plaintiff, because Defendant has “assist[ed] Adyen in intercepting and indefinitely storing this sensitive information” by integrating Adyen’s platform into its website, Defendant is culpable for its facilitation of this process. (*Id.* ¶ 39.)

II. LEGAL STANDARD

Federal Rule of Civil Procedure 8(a)(2) requires a complaint to include “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). A complaint that fails to meet this standard may be dismissed pursuant to Rule 12(b)(6). *See* Fed. R. Civ. P. 12(b)(6). To overcome a Rule 12(b)(6) motion to dismiss after the Supreme Court’s decisions in *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atlantic Corporation v. Twombly*, 550 U.S. 544 (2007), a plaintiff’s “factual allegations [in the complaint] ‘must . . . suggest that the claim has at least a plausible chance of success.’” *Levitt v. Yelp! Inc.*, 765 F.3d 1123, 1135

(9th Cir. 2014).

The court “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008). But “allegations in a complaint . . . may not simply recite the elements of a cause of action [and] must contain sufficient allegations of underlying facts to give fair notice and to enable the opposing party to defend itself effectively.” *Levitt*, 765 F.3d at 1135 (quoting *Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014)). “A claim has facial plausibility when the Plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Iqbal*, 556 U.S. at 678. “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (quoting *Twombly*, 550 U.S. at 556).

III. DISCUSSION

A. California Penal Code Section 631(a)

To plead a violation of § 631(a), Plaintiff must allege sufficient facts to show that Defendant either (1) engaged in intentional wiretapping; (2) willfully read “the contents or meaning” of a communication without consent; (3) attempted to use or communicate information obtained as a result of engaging in the previous two activities; or (4) aided another in any of the previous three activities. Cal. Penal Code § 631(a). Plaintiff’s theory is that Defendant is liable under the fourth clause of § 631(a) because Defendant “aided, agreed with, and conspired with Adyen to track and intercept Plaintiff’s and Class Members’ internet communications while accessing www.yeti.com.” (FAC ¶ 55.) Although Plaintiff alleges a sufficient basis for Adyen’s liability, the First Amended Complaint as currently pled does not allege sufficient facts to hold Defendant derivatively liable for Adyen’s conduct.

1. Adyen’s Alleged Violation of Section 631(a)

To establish Defendant’s derivative liability under the fourth clause of § 631(a), Plaintiff must first show that Adyen engaged in conduct prohibited by the first, second, or third clause.

Plaintiff sufficiently alleged that Adyen’s conduct violated both the second and third clauses of § 631(a). Either violation is sufficient as the predicate for Defendant’s derivative liability.

The second clause of § 631(a) has three requirements: (1) the “absence of consent” of all parties to the communication; (2) eavesdropping by a third-party nonparticipant to the communication; and (3) an interception of the communication “while in transit.” *Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751, 756 (N.D. Cal. 2023). Defendant does not dispute that Plaintiff has adequately alleged the communication was intercepted while in transit. Plaintiff also plausibly alleges that Adyen acted as a third-party nonparticipant to the communication and that Plaintiff did not consent to Adyen’s eavesdropping.

Starting with the third-party nonparticipant requirement, Adyen’s status as a nonparty to the communication turns on whether Adyen’s conduct was “sufficiently independent” from Defendant to be considered a distinct party. *Licea v. Cinmar, LLC*, 659 F. Supp. 3d 1096, 1109 (C.D. Cal. 2023). To make this determination, “courts have been instructed to analyze whether the technology (or actor) behaves more akin to a tape recorder utilized by the party to the conversation or as an eavesdropper ‘pressing up against the door to listen to a conversation.’” *Id.* at 1107 (quoting *Revitch v. New Moosejaw, LLC*, No. 18-cv-06827, 2019 WL 5485330, at *2 (N.D. Cal. Oct. 23, 2019)). Based on Plaintiff’s complaint, there are sufficient allegations that Adyen does not simply collect consumers’ personally identifiable and financial information in order to process payments and facilitate transactions on Defendant’s website. Rather, Plaintiff sufficiently alleges that Adyen collected Plaintiff’s information “to monetize and market [their] services to Defendant and other merchants within Adyen’s network,” which is a distinct commercial purpose. (FAC ¶ 8.) Defendant does not argue that Adyen benefits from party status. Thus, based on the allegations that Adyen acts in an independent manner, Adyen is a third-party nonparticipant to the communication.

Plaintiff also sufficiently alleges that she did not consent to Adyen’s eavesdropping. Defendant argues that its Terms and Privacy Policy “expressly disclosed to Plaintiff and other YETI users that the information she provided at payment checkout would be shared with third-

party service providers (like Adyen).” (Dkt. No. 23-1 at 11.)¹ But under California law, consumers must have actually or constructively consented to be bound by these contractual terms. *Allen v. Shutterfly, Inc.*, No. 20-cv-02448, 2020 WL 5517172, at *6 (N. D. Cal. Sept. 14, 2020). “[A]n enforceable agreement may be found where (1) the website provides reasonably conspicuous notice of the terms to which the consumer will be bound; and (2) the consumer takes some action, such as clicking a button or checking a box, that unambiguously manifests his or her assent to those terms.” *Oberstein v. Live Nation Ent., Inc.*, 60 F.4th 505, 515 (9th Cir. 2023). Based on how the Privacy Policy and Terms are displayed on Defendant’s website, consent cannot be inferred.

Most internet contracts are “clickwrap” agreements or “browsewrap” agreements. *Allen*, 2020 WL 5517172, at *2. Clickwrap agreements require users to click an “I agree” button after being provided with the website’s terms and conditions of use. Browsewrap agreements display a website’s terms and conditions of use via a hyperlink, usually at the bottom of the screen. Defendant argues that its website does both.² According to Defendant, its Privacy Policy is included “on a bright white pop-up banner highlighted on the page.” (Dkt. No. 23-1 at 8.) Defendant also argues that it makes its Privacy Policy available “on its home page via a link in white text on a dark blue background.” (*Id.*)

Defendant’s inclusion of the pop-up banner does not constitute a clickwrap agreement. The pop-up banner may be reasonably conspicuous to satisfy the first requirement of the test articulated in *Oberstein*. However, Defendant’s pop-up banner does not require individuals to click an “I agree” button, nor does it include any language to imply that by proceeding to use the website, users reasonably consent to Defendant’s terms and conditions of use. Therefore, the

¹ Citations to page numbers refer to the ECF pagination.

² Defendant filed a Request for Judicial Notice and Incorporation by Reference of its Privacy Policy (Exhibit A of the Declaration of Hannah Tucker), a screenshot of its cookie banner that appears on the bottom of Defendant’s home page (Exhibit B of the Declaration of Hannah Tucker), and its Terms and Conditions of Use (Exhibit C of the Declaration of Hannah Tucker). (Dkt. No. 23-6.) These documents are incorporated by reference because Plaintiff’s complaint makes allegations regarding the existence and content of the Privacy Policy and Terms. (FAC ¶¶ 35-37.)

pop-up banner cannot be treated as a traditional clickwrap agreement that renders the website's terms and conditions of use enforceable against Plaintiff or other users.

Nor do the pop-up banner or link on the Defendant's homepage suffice to provide the requisite "constructive assent" for a browsewrap agreement. *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014). Courts consider "the conspicuous placement of the 'Terms of Use' hyperlink, other notices given to users of the terms of use, and the website's general design" in determining "whether a reasonably prudent user would have inquiry notice of a browsewrap agreement." *Id.* at 1177. The Privacy Policy and Terms of Use may be sufficiently conspicuous on Defendant's website as to satisfy the first requirement articulated in *Oberstein*. But where a website "makes its terms of use available via a conspicuous hyperlink on every page of the website *but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent*, even close proximity to relevant buttons users must click on—without more—is insufficient to give rise to constructive notice." *Id.* at 1179 (emphasis added). Defendant's website does not require additional action by users to demonstrate assent and does not conspicuously notify them that continuing to use to website constitutes assent to the Privacy Policy and Terms of Use. Therefore, Plaintiff's consent cannot be inferred from the record presented by Defendant.

Accordingly, Plaintiff has sufficiently alleged that Adyen's conduct violated the second clause of § 631(a). Moreover, for the same reasons explained above, Plaintiff has also sufficiently alleged a separate basis for derivative liability: that Adyen's conduct violated the third clause of § 631(a). As a result of engaging in the above-described conduct, Adyen also allegedly *used* the information it collected "to monetize and market [their] services to Defendant and other merchants within Adyen's network." (FAC ¶ 8.) Defendant does not separately contest this point, beyond the arguments addressed above.

2. Defendant's Liability for Adyen's Alleged Violation of § 631(a)

Although Plaintiff has sufficiently alleged a basis to believe that Adyen violated the second and third clauses of § 631(a), Plaintiff has not adequately alleged a basis for Defendant's

derivative liability. Plaintiff has not plausibly alleged that Defendant aided, agreed with, employed, or conspired with Adyen “to unlawfully do, or permit, or cause to be done any of the acts” that Adyen undertook in violation of § 631(a). The parties disagree about the requirements to allege liability under this clause. According to Defendant, the fourth clause imputes a scienter requirement, which mirrors the requirements for establishing conspiracy or accomplice liability. In this view, Plaintiff must allege that Defendant acted with “specific intent to commit the unlawful acts” or with “knowledge of ‘the unlawful purpose and inten[t] to help [Adyen] accomplish that purpose.’” (Dkt. No. 23-1 at 14 (citing *People v. Swain*, 909 P.2d 994 (Cal. 1996) and quoting *People v. Lee*, 74 P.3d 176 (Cal. 2003)).) Plaintiff, on the other hand, argues that “[t]he legislature’s use of the terms ‘aids,’ ‘agrees with,’ and ‘employs’ indicates that CIPA § 631(a) was mean[t] to apply to a much broader swath of non-criminal conduct, regardless of ‘specific intent.’” (Dkt. No. 24 at 12 (quoting *Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1129-30 (S.D. Cal. 2023)).)

The statute does not necessarily incorporate the common law requirement for aiding and abetting simply because it contemplates liability where an individual or entity provides “aid.” See *Cousin*, 681 F. Supp. 3d at 1130 (“Defendant’s contention that ‘aids’ means ‘aiding and abetting’ ignores the ‘agrees with, employs, or conspires with’ language of the clause.”). But see, e.g., *Esparza v. UAG Escondido AI Inc.*, No. 23-cv-0102, 2024 WL 559241, at *6 (S.D. Cal. Feb. 12, 2024) (imputing the aiding and abetting standard from common law as the scienter requirement because none was expressly provided for in the statute).

However, other language in § 631(a)’s fourth clause does require some level of knowledge and intent. That clause prohibits a defendant from aiding, agreeing with, or employing a third party “*to* unlawfully do, or permit, or cause” the third party to act in violation of the wiretapping statute. Cal. Pen. Code § 631(a) (emphasis added). That language indicates that the defendant must be acting with the third party *in order to* have the third party perform acts that violate the statute. At the very least, that requires both knowledge of the conduct that will violate the statute and a purpose of aiding, agreeing with, or employing the third party to

commit those acts. By its plain terms, that statutory language does not cover, for example, a defendant who properly and lawfully provides information or access to a third party without any knowledge or intent that the third party will use the information in a manner that violates the statute. Such a defendant has not aided, agreed with, or employed the third party *to* perform acts that violate the wiretapping statute.

Plaintiff fails to allege facts sufficient to show the requisite knowledge and intent. In her complaint, Plaintiff alleges that Defendant was “aware of the purposes for which Adyen collects consumers’ sensitive information because Defendant is knowledgeable of and benefitting from Adyen’s fraud prevention services.” (FAC ¶ 41.) Plaintiff also alleges that Defendant “assists Adyen in intercepting and indefinitely storing this sensitive information.” (*Id.* ¶ 39.) Those conclusory allegations do not contain sufficient facts for the Court to draw a plausible inference that Defendant knowingly agreed with or employed Adyen to engage in conduct that violated the wiretapping statute. Without further information, the Court cannot plausibly infer from Defendant’s use of Adyen’s fraud prevention services alone that Defendant *knew* that Adyen’s services were based on its allegedly illegal interception and storing of financial information, collected during Adyen’s online processing of customers’ purchases. Plaintiff alleges that Adyen’s fraud detection software uses “network-wide insights” that include attributes based on email, card information, and delivery address, but does not indicate how Defendant would know those “insights” came from Adyen’s processing of payments from Defendant’s website. (*Id.* ¶ 28.) Accordingly, the motion to dismiss this claim is granted.

B. California Penal Code Section 632

To state a claim under § 632, Plaintiff must show there was (1) an electronic recording of (2) a confidential communication and (3) all parties did not consent. *Turner v. Nuance Commc’ns, Inc.*, No. 22-cv-05827, 2024 WL 2750017, at *4 (N.D. Cal. May 28, 2024). It is not disputed that there was an electronic recording of the communication. However, Defendant argues that the communication was not confidential, that Plaintiff did consent to the recording, and that derivative liability cannot be imposed under § 632.

First, Plaintiff has plausibly alleged that the communications were confidential. A communication is confidential under § 632 if a party “has an objectively reasonable expectation that the conversation is not being overheard or recorded.” *Flanagan v. Flanagan*, 41 P. 3d 575, 576 (Cal. 2002) (endorsing this standard). This is a “fact-intensive inquiry” that is often too difficult to resolve at the pleadings stage. *Brown v. Google LLC*, 685 F. Supp. 3d 909, 937 (N.D. Cal. 2023); *see also Lieberman v. KCOP Television, Inc.*, 1 Cal. Rptr. 3d 536, 545 (Ct. App. 2003) (“It is for the jury to decide whether under the circumstances presented [Plaintiff] could have *reasonably* expected that the communications were private.”). Plaintiff alleged that she “reasonably expected that Defendant would keep [her personally identifiable and credit card] information private and not disclose it to third parties.” (FAC ¶ 7.) Whether the expectation of privacy was reasonable in this particular circumstance is a fact-specific inquiry, but Plaintiff has plausibly alleged that the sensitive financial information being recorded is the type that could be reasonably considered confidential. Thus, the second element is met.

Second, for the reasons provided above, Plaintiff plausibly alleged that she did not consent to the recording. The analysis under § 632 is identical to the analysis under § 631(a). Neither Defendant’s pop-up banner nor its link on its homepage render the Privacy Policy or Terms of Use enforceable against Plaintiff. Although these terms and conditions of use may have been conspicuously displayed, Plaintiff did not manifest her assent either through clicking an “I agree” button or by affirmatively using the website after being told that such use would constitute assent to those terms. Therefore, the third element is also met.

However, Plaintiff again has not alleged sufficient facts to support a plausible inference of derivative liability. Unlike the fourth clause of California Penal Code § 631(a), the text of Penal Code § 632 does not expressly provide for derivative liability. However, under Penal Code § 31, “[a]ll persons concerned in the commission of a crime . . . or [who] aid and abet in its commission . . . are principals in any crime so committed.” *See Vera v. O’Keefe*, 791 F. Supp. 2d 959, 963 (S.D. Cal. 2011). In applying this principle to civil lawsuits for violations of Penal Code § 632, courts have imputed the civil liability standard for aiding and abetting to determine

the scope of derivative liability. At common law, a person aids and abets the commission of a crime when they “(a) know the other’s conduct constitutes a breach of duty and give substantial assistance or encouragement to the other to so act or (b) give substantial assistance to the other in accomplishing a tortious result and the person’s own conduct, separately considered, constitutes a breach of duty to the third person.” *Esparza*, 2024 WL 559241, at *6 (citing *Saunders v. Superior Court*, 33 Cal. Rptr. 2d 438, 446 (Ct. App. 1994)). Thus, to establish liability, Defendant must have knowledge of the other’s conduct and must have provided substantial assistance. For the same reasons as stated above, Plaintiff did not plead sufficient facts to support a plausible inference that Defendant had knowledge of Adyen’s conduct violating the statute, let alone had an intent or purpose of aiding it substantially. As such, the motion to dismiss this claim is granted.

C. Invasion of Privacy Under the California Constitution

“The California Constitution sets a ‘high bar’ for establishing an invasion of privacy claim.” *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014) (citation omitted). Plaintiff must establish three elements: “(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.” *Hill v. Nat’l Collegiate Athletic Ass’n*, 26 Cal. Rptr. 2d 834, 859 (Ct. App. 1994). Under the third prong, “[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.” *Id.* at 857. Plaintiff plausibly alleged the first two elements. However, Plaintiff does not establish that Defendant’s conduct amounted to a serious invasion of privacy.

Defendant does not appear to dispute that Plaintiff has a legally protected privacy interest in her personally identifiable and financial information. Under the California Constitution, an individual has a legally protected privacy interest in “precluding the dissemination or misuse of sensitive and confidential information.” *Id.* at 856. “A particular class of information is private when well-established social norms recognize the need to maximize individual control over its

dissemination and use.” *Id.* Courts have recognized that individuals retain a privacy interest in their personally identifiable information, including their name, address, and phone number. *See, e.g., Padron v. Lara*, No. 1:16-cv-00549, 2018 WL 2213462, at *13 (E.D. Cal. May 11, 2018). Sensitive financial information also falls into this category. Plaintiff alleges that Defendant collected her “personally identifiable information” and “confidential communications that contain[ed] [her] sensitive financial information,” including credit card number, card issuer, expiration date, and CVC. (FAC ¶¶ 3, 6, 7.) Accordingly, Plaintiff has sufficiently established that she has a legally protected privacy interest in the type of information that she provided to Defendant. The first element is met.

However, despite the collection of Plaintiff’s personally identifiable and financial information, Defendant argues that Plaintiff has no reasonable expectation of privacy “as to YETI’s *fully disclosed* sharing with its payment processor, Adyen, of the information Plaintiff included in the ‘form fields’ for her purchase.” (Dkt. No. 23-1 at 18 (emphasis added).) But “[w]hether a party has a reasonable expectation of privacy is a context-specific inquiry that should not be adjudicated as a matter of law unless the undisputed material facts show no reasonable expectation of privacy.” *Padron*, 2018 WL 2213462, at *9 (internal quotations and citations omitted). In this case, the inquiry not only turns on whether Plaintiff should have reasonably expected that YETI would share her information with Adyen for payment processing, but also on whether she should have reasonably expected her information to be integrated into Adyen’s broader “fraud prevention network,” which is used to provide “additional services to merchants.” (FAC ¶¶ 25-26.) This is precisely the type of fact-specific inquiry that cannot be decided on the pleadings. At this stage, Plaintiff alleges that she did not consent to her sensitive information “being disclosed and used in this manner,” which is sufficient to establish the second element of the claim. (*Id.* ¶ 42.)

Defendant argues that “consumers do not have a reasonable expectation of privacy over their commercial activity on the Internet.” (Dkt. No. 23-1 at 18.) And, indeed, courts have recognized that consumers do not always retain a reasonable expectation of privacy in their

information once that information is voluntarily disclosed during the course of ordinary online commercial activity. *See, e.g., D'Angelo v. Penny OpCo, LLC*, No. 23-cv-0981, 2023 WL 7006793, at *11 (S.D. Cal. Oct. 24, 2023) (finding no reasonable expectation of privacy in online chats with customer service representative); *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503, 525 (C.D. Cal. 2011) (no reasonable expectation of privacy in third party's capturing of user's "mouse clicks," "keystrokes," "payment card information," etc.); *Thomas v. Papa Johns Int'l, Inc.*, No. 22-cv-2012, 2024 WL 2060140, at *4-5 (S.D. Cal. May 8, 2024) (no reasonable expectation of privacy in recording of "mouse movements," "clicks," "keystrokes," and "name, address, credit card number(s), and billing information."). But these cases do not reflect a blanket presumption that no reasonable expectation of privacy exists when engaging in commercial transactions over the Internet. *Thomas*, 2024 WL 2060140, at *2 ("This is not to say there can never be a reasonable expectation of privacy over internet activity."). And each of these cases is distinguishable from the facts presented by Plaintiff. In *D'Angelo*, no sensitive financial information was being recorded. And in *Saleh* and *Thomas*, there is no allegation that the information turned over to the third party was being used for a distinct and independent commercial purpose. Thus, these cases do not decide the issue that must be resolved here. Plaintiff has plausibly alleged that her expectation of privacy in her information was reasonable, and therefore, the second element is sufficiently pled.

In terms of the third element, Plaintiff fails to plausibly allege facts from which the Court could plausibly infer that Defendant's conduct is so egregious as to constitute a "serious invasion of privacy." Courts recognize that the offensiveness of the conduct typically cannot be resolved at the pleading stage, as this is also a fact-specific inquiry. *See, e.g., In re Google Location Hist. Litig.*, 514 F. Supp. 3d 1147, 1157-58 (N.D. Cal. 2021). However, where the conduct amounts to "routine commercial behavior," the third element is not met. *See, e.g., Folgelstrom v. Lamp Plus, Inc.*, 125 Cal. Rptr. 3d 260, 265 (Ct. App. 2011). Whether Defendant's conduct was highly offensive turns on what specifically Plaintiff is alleging Defendant knew. If Defendant simply engaged Adyen to undertake ordinary payment processing responsibilities, that conduct alone

cannot amount to a serious invasion of Plaintiff's privacy. However, if Defendant was aware of Adyen's usage of the personal information for additional purposes, this may present a plausible allegation that Defendant's conduct was sufficiently egregious to survive a motion to dismiss. As discussed above, Plaintiff has not alleged facts sufficient to allow a plausible inference regarding Defendant's knowledge of Adyen's acts. Accordingly, the motion to dismiss this claim is granted.

* * *

For the reasons described above, Defendant's motion to dismiss is **GRANTED** as to all claims. Since the Court cannot conclude that amendment would be futile, dismissal is granted with leave to amend. If Plaintiff wishes to file a Second Amended Complaint correcting the deficiencies identified above, counsel shall do so within **21 days of the date of this Order**. The Second Amended Complaint may not add new claims or parties, or otherwise change the allegations except to correct the identified deficiencies, absent leave of the Court or stipulation by the parties pursuant to Federal Rule of Civil Procedure 15. If no Second Amended Complaint is filed by that date, the First Amended Complaint will remain dismissed, judgment will be entered in favor of Defendants, and the case will be closed.

IT IS SO ORDERED.

Dated: October 21, 2024



RITA F. LIN
United States District Judge